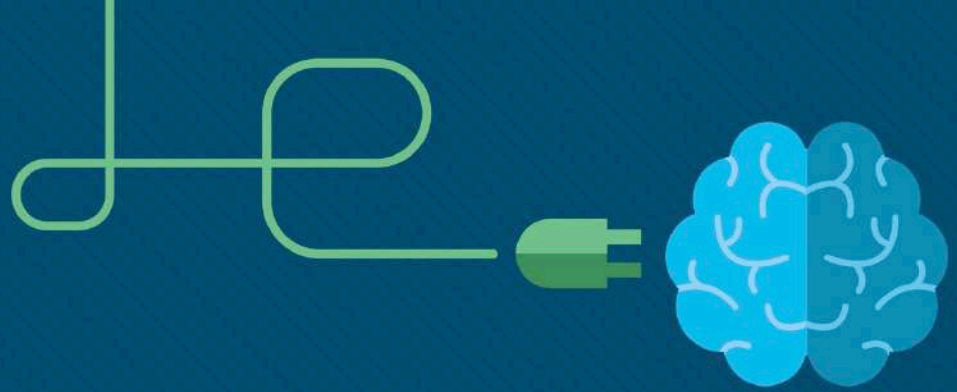
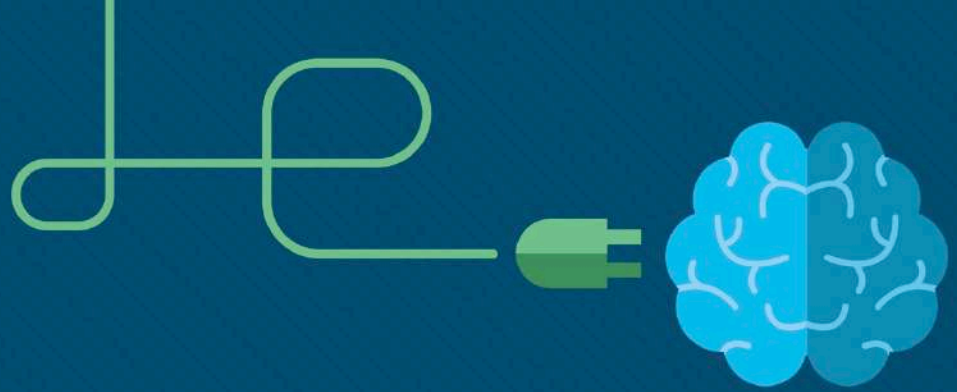


Capítulo 4: Proteção da empresa

Material do instrutor

Introdução ao Cybersecurity v2.1



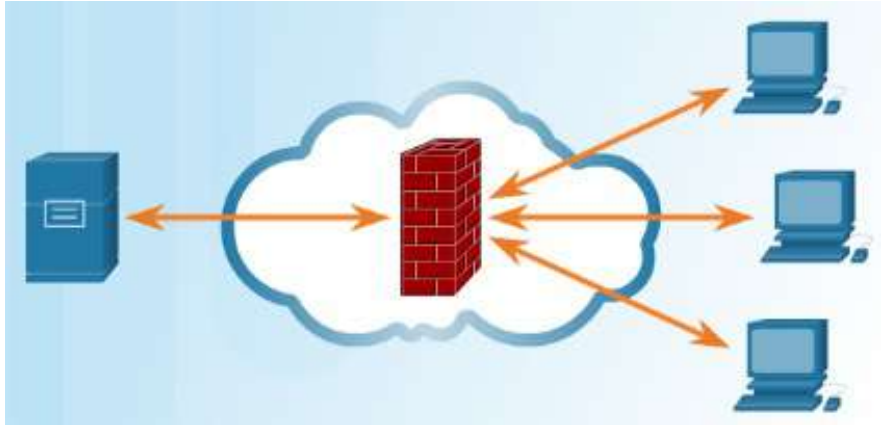
Capítulo 4: Proteção da empresa

Introdução ao Cybersecurity v2.1

4.1 Firewalls

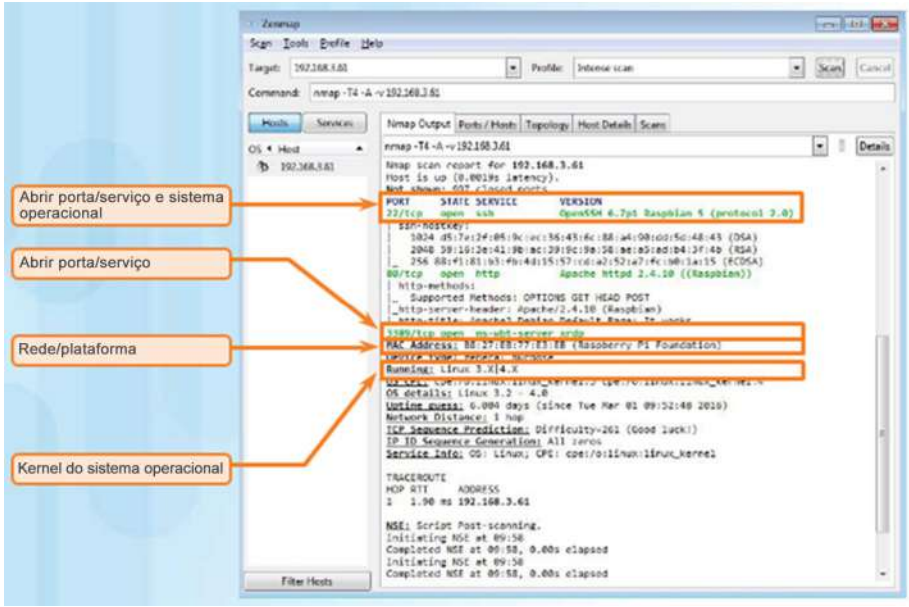
Tipos de Firewall

- Controla ou filtra as comunicações de entrada ou saída em uma rede ou dispositivo
- Tipos de firewall comuns
  - **Firewall de camada de rede** – endereços IP de origem e destino
  - **Firewall de camada de transporte** – portas de dados de origem e destino, estados de conexão
  - **Firewall de camada de aplicação** – aplicativo, programa ou serviço
  - **Firewall de aplicação com reconhecimento de contexto** – usuário, dispositivo, função, tipo de aplicativo e perfil de ameaça
  - **Servidor proxy** – solicitações de conteúdo da Web
  - **Servidor proxy reverso** – protege, esconde, descarrega e distribui o acesso a servidores da Web
  - **Firewall Network Address Translation (NAT)** – oculta ou disfarça os endereços privados de hosts de rede
  - **Firewall baseado em host** – filtragem de portas e chamadas de serviço do sistema em um sistema operacional de computador único



Varredura de porta

- Processo de sondagem de um computador, servidor ou outro host de rede para identificar portas abertas.
- Os números de porta são atribuídos a cada aplicativo em execução em um dispositivo.
- Ferramenta de reconhecimento para identificar os sistemas operacionais e serviços em execução
  - Nmap – uma ferramenta de varredura de portas
- Respostas comuns:
  - **Aberta ou aceita** – um serviço está escutando na porta.
  - **Fechada, negada ou não escutando** – conexões serão negadas à porta.
  - **Filtrada, descartada ou bloqueada** – não houve resposta do host.

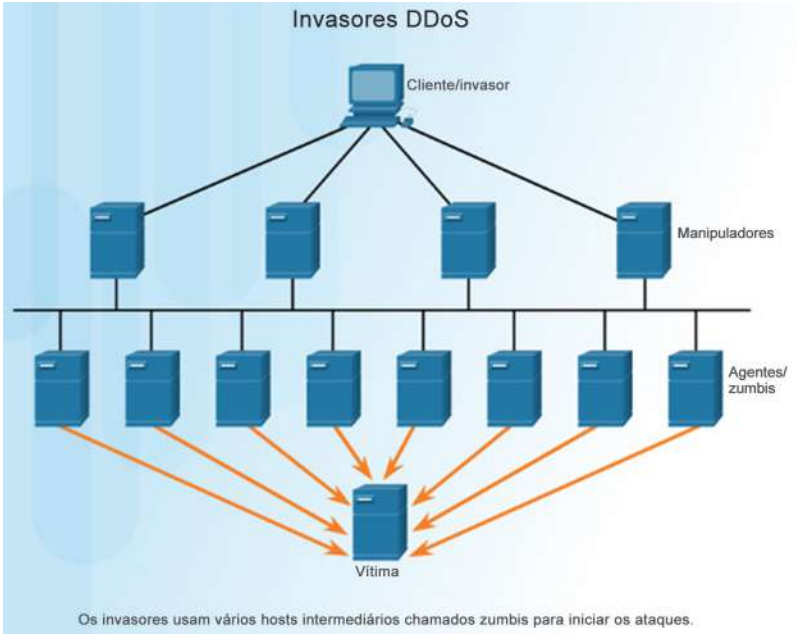


Equipamentos de segurança

- Os equipamentos de segurança enquadram-se nestas categorias gerais:
  - **Roteadores** – podem ter muitos recursos de firewall: filtragem de tráfego, IPS, criptografia e VPN.
  - **Firewalls** – também pode ter a capacidade de roteador, gerenciamento de rede e análises avançados.
  - **IPS** – dedicado à prevenção de intrusões.
  - **VPN** – projetados para tunelamento criptografado seguro.
  - **Malware/antivírus** – o Cisco Advanced Malware Protection (AMP) vem em roteadores Cisco Next Generation, firewalls, dispositivos IPS, dispositivos de segurança da Web e e-mail e também pode ser instalado como um software em computadores.
  - **Outros dispositivos de segurança** – inclui dispositivos de segurança de Web e e-mail, dispositivos de descriptografia, servidores de controle de acesso para cliente e sistemas de gerenciamento de segurança.

Detecção de ataques em tempo real

- ataque de dia zero
  - Um hacker explora uma falha em uma parte do software antes do criador poder corrigi-la.
- **Varredura em tempo real da borda para o endpoint**
  - varredura ativa de ataques usando firewall e dispositivos de rede IDS/IPS.
  - detecção com conexões a centros on-line de ameaça global
  - detecção de anomalias de rede usando a detecção de comportamento e análise baseada em contexto
- **Ataques de DDoS e resposta em tempo real**
  - DDoS, uma das maiores ameaças de ataque, pode paralisar os servidores da Internet e a disponibilidade de rede.
  - A DDoS origina centenas, ou milhares de hosts zumbis, e os ataques aparecem como tráfego legítimo.



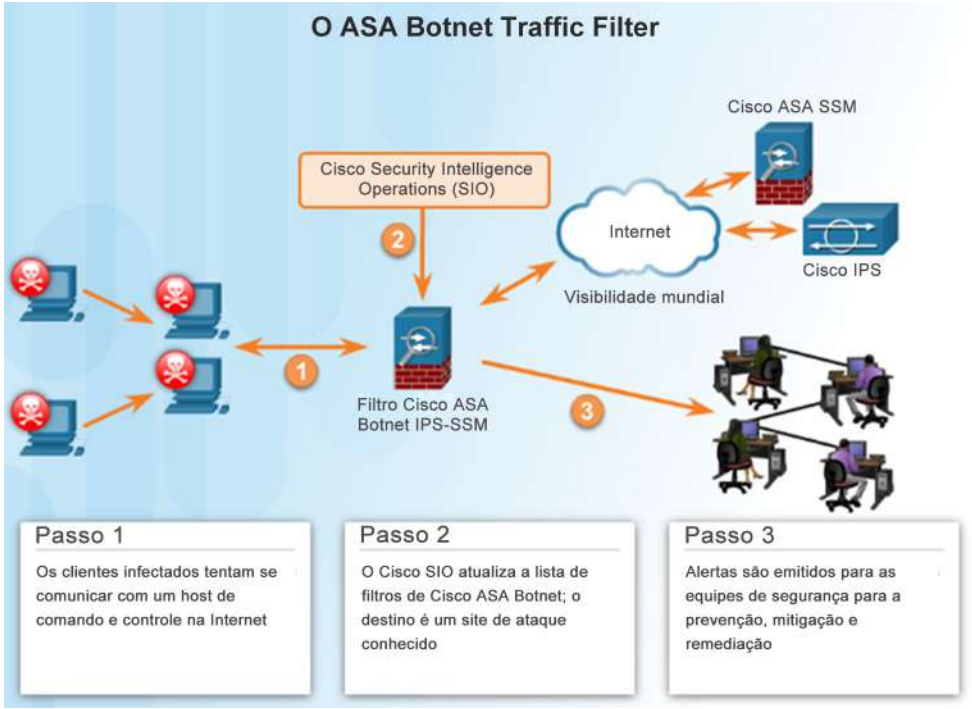
Melhores práticas de segurança

- **Algumas melhores práticas de segurança publicadas:**
  - **Realizar a avaliação de risco** – Saber o valor do que você está protegendo ajudará a justificar as despesas de segurança.
  - **Criar uma política de segurança** – Criar uma política que define claramente as regras da empresa, os deveres e as expectativas do trabalho.
  - **Medidas de segurança física** – Restringir o acesso a racks de rede, locais de servidor, bem como supressão de fogo.
  - **Medidas de segurança de recursos humanos** – Os antecedentes dos funcionários devem ser devidamente pesquisados.
  - **Executar e testar backups** – Fazer backups regulares e teste de recuperação de dados de backups.
  - **Manter atualizações e patches de segurança** – Atualizar regularmente o servidor e os sistemas operacionais e programas de dispositivos de rede e do cliente.
  - **Empregar controles de acesso** – Configurar funções de usuário e níveis de privilégio, bem como autenticação forte ao usuário.
  - **Testar regularmente a resposta a incidentes** – Empregar uma equipe de resposta a incidentes e testar cenários de resposta a emergências.
  - **Implementar uma rede de monitoramento, análise e ferramenta de gerenciamento** – Escolher uma solução de gerenciamento de segurança que se integra a outras tecnologias.
  - **Implementar dispositivos de segurança de rede** – Use roteadores next generation, firewalls e outros dispositivos de segurança.
  - **Implementar uma solução abrangente de segurança de endpoint** – Use software antivírus e antimalware de nível corporativo.
  - **Treinar os usuários** – Treinar os usuários e funcionários nos procedimentos de segurança.
  - **Criptografar dados** – Criptografar todos os dados confidenciais da empresa, incluindo e-mail.

4.2 Abordagem comportamental à segurança cibernética

Botnet

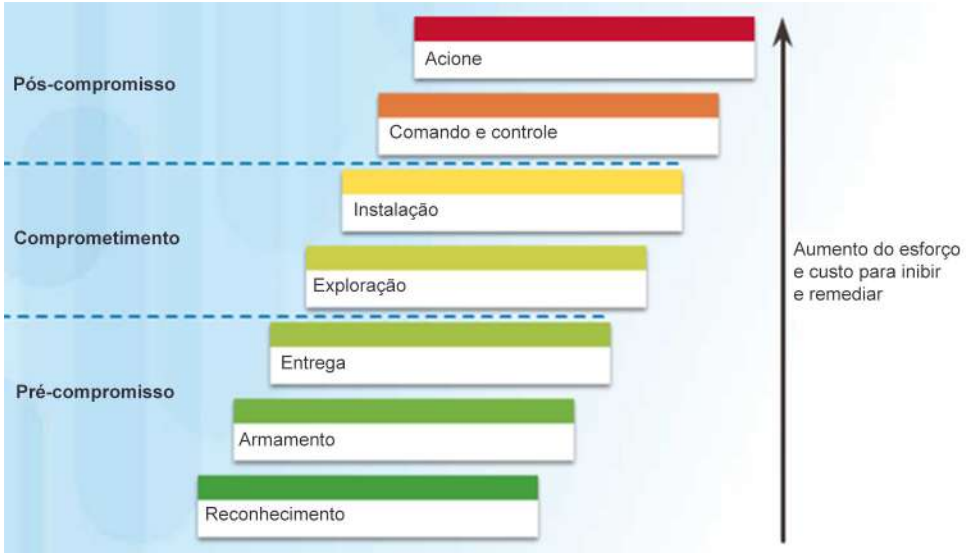
- Botnet
  - Um grupo de bots se conectam pela Internet
  - Controlado por indivíduos ou grupos mal-intencionados
- Bot
  - Normalmente é infectado por visitar um site, abrir um anexo de e-mail ou abrir um arquivo de mídia infectado.



A Kill Chain na defesa cibernética

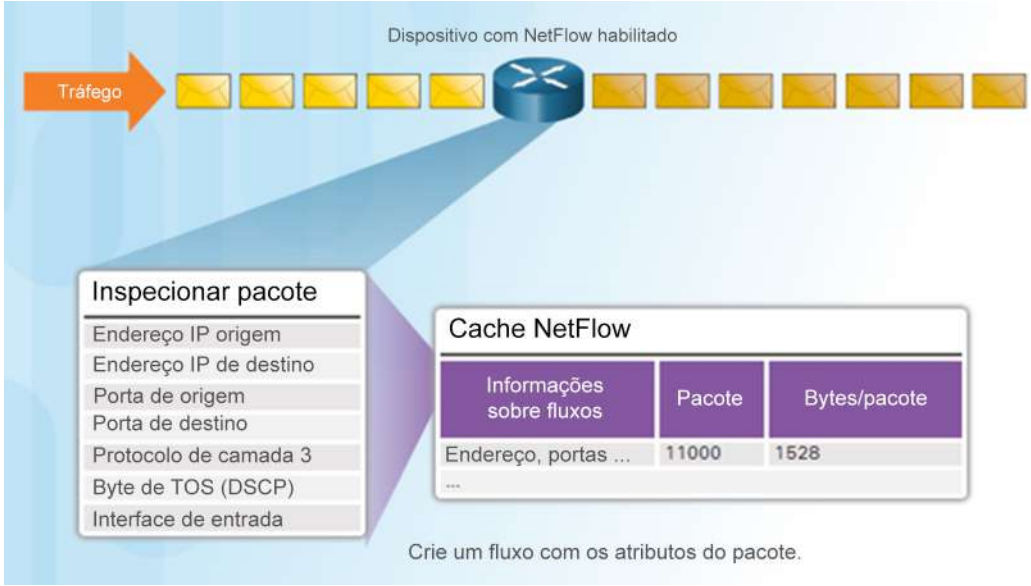
Kill Chain consiste nas etapas de um ataque de sistemas de informação.

1. **Reconhecimento** – Reúne informações
2. **Armamento** – Cria exploit e payload mal-intencionados direcionados
3. **Entrega** – Envia o exploit e o payload mal-intencionado para o destino
4. **Exploração** – Executa o exploit
5. **Instalação** – Instala o malware e backdoors
6. **Comando e controle** – Controle remoto de um canal de comando e controle ou servidor.
7. **Ação** – Executa ações mal-intencionadas ou ataques adicionais em outros dispositivos



Netflow

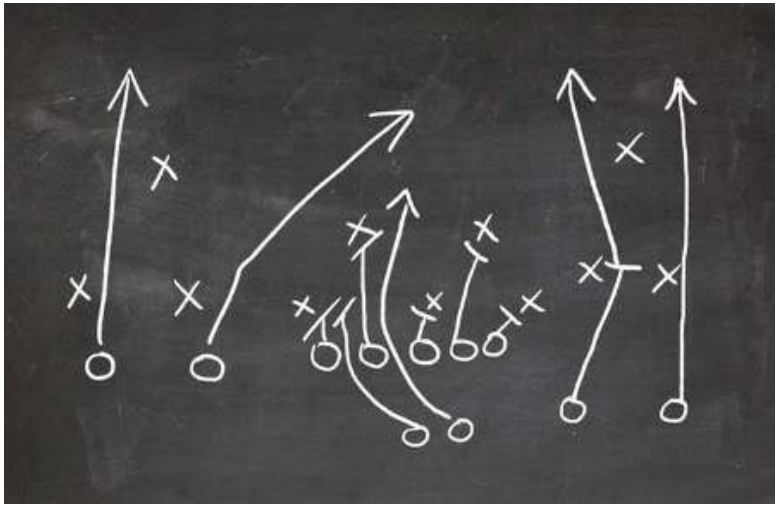
- Coleta informações sobre dados fluindo por uma rede.
- Componentes importantes na análise e detecção baseada em comportamento.
- Estabelece comportamentos de parâmetro



4.3 Abordagem da Cisco à segurança cibernética

Cartilha de segurança

- Coleção de consultas repetitivas contra fontes de dados de evento de segurança que levam à detecção de incidentes e resposta.
- O que ela precisa fazer?
  - Detectar máquinas infectadas com malware.
  - Detectar atividades suspeitas na rede.
  - Detectar tentativas de autenticação irregulares.
  - Descrever e compreender o tráfego de entrada e de saída.
  - Fornecer informações resumidas, incluindo tendências, estatísticas e contagens.
  - Dar acesso útil e rápido a estatísticas e métricas.
  - Correlacionar eventos em todas as fontes de dados relevantes.



IDS e IPS

- IDS – Sistema de detecção de invasão
  - Geralmente fica off-line
  - Não impede ataques
  - Detecta, registra e relata
- IPS – Sistema de prevenção de invasões
  - Capacidade de bloquear ou negar o tráfego com base em uma regra de correspondência ou assinatura positiva.
- Sistema IDS/IPS
  - Snort
  - Sourcefire (Cisco)


CISCO